Final – August 29, 2006

テロ行為防止のための税関産業界提携プログラム (C-TPAT)
セキュリティ基準
外国の製造業者

このセキュリティ最低基準は、グローバル・サプライチェーンにテロリストやテロ活動の介在を招きかねない紛失、盗難、密輸などを最小限に抑え、サプライチェーンを適正化するための効果的なセキュリティ措置を制定するための土台として提供されています。内部共謀を通して世界の通商を狙う犯罪組織の範囲を見極めるには、企業、特に外国の製造業者による自社セキュリティ措置の改善が必要です。

少なくとも 1 年に 1 度、あるいは厳重警戒、セキュリティ違反・事故の時期などの状況に応じて、外国の製造業者は以下の C-TPAT セキュリティ基準に基づく自社国際サプライチェーンの包括的なアセスメントを実施しなければなりません。外国の製造業者が、他の外国施設や倉庫などのサプライチェーンの要素を外注または下請けにに出す場合、外国の製造業者はその事業提携会社の協力を得て、自分達のサプライチェーン全体に適切なセキュリティ対策が実施されていることを確実にしなければなりません。C-TPAT の目的におけるサプライチェーンとは、ポイント・オブ・オリジン(原産地：製造業者/仕入業者/ベンダー)からポイント・オブ・ティストリビューション(流通点)までを意味し、C-TPAT メンバーが使用している多様なビジネスモデルがあることも理解しています。

C-TPAT は国際サプライチェーンとセキュリティ対策の複雑さを理解し、リスクに応じたセキュリティ方策の応用と実施を奨励します。[1] *従って、このプログラムはメンバーのビジネスモデルに応じてセキュリティプランの柔軟性とカスタマイズを認めています。*

本書を通して言及されるセキュリティ対策は、外国の製造業者のサプライチェーンを通してそのリスクに合わせて実施され維持されなければなりません。[2]

---

[1] 外国の製造業者は、そのビジネスモデルに基づくサプライチェーン全体のリスクを判断するための文書化された検証可能なプロセスを定めていなければなりません。(例：数量、原産国、経路、C-TPAT のメンバーかどうか、潜在的なテロの脅威という公開情報、セキュリティ対策不足、過去のセキュリティ問題など)

[2] 外国の製造業者は、そのビジネスモデルに基づくサプライチェーン全体のリスクを判断するための文書化された検証可能なプロセスを定めていなければなりません。(例：数量、原産国、経路、C-TPAT のメンバーかどうか、潜在的なテロの脅威という公開情報など)

事業提携会社の必要条件

外国の製造業者は、運送会社、その他(部品や原材料の仕入先などの)製造業者、製品仕入先、業者などの事業提携会社の選定に関する文書化した検証可能なプロセスを持たなければなりません。

- **セキュリティ手続き**

  C-TPAT 認証取得資格のある(運送会社、港湾、ターミナル、仲介業者、混載業者などの)事業提携会社については、外国の製造業者はこれらの事業提携会社が C-TPAT 認証取得済みかどうかを示す書類(C-TPAT 証明書、SVI 番号など)を持っていなければなりません。

  C-TPAT 認証取得資格のない事業提携会社については、外国の製造業者は、その事業提携会社に文書または電子的に確認させることで C-TPAT のセキュリティ基準を満たしていることを証明させる必要があります。(例：契約上の義務、事業提携会社の重役が遵守を証明した手紙、C-TPAT のセキュリティ基準、または外国税関当局が実施している同等の世界税関機構(WCO)認証セキュリティ制度を遵守していることを証明する事業提携会社からの文書、あるいは外国の製造業者からのセキュリティ質問書に回答することによって)。文書化されたリスクアセスメント・ プロセスに基づいて、C-TPAT 参加資格のない事業提携会社に対して外国の製造業者は C-TPAT セキュリティ基準遵守の証明を要求することが必要になります。

- **ポイント・ オブ・ オリジン (原産地)**

  外国の製造業者は、ポイント・ オブ・ オリジン(原産地)、組立地、または製造地における出荷物の完全性を強化するために、事業提携会社に対して C-TPAT セキュリティ基準に一致したセキュリティプロセスと手続きを策定させなければなりません。リスクに応じて事業提携会社のプロセスや施設の検討を定期的に行い、外国の製造業者が要求するセキュリティ基準を維持させなければなりません。

- **外国税関当局のサプライチェーン保全制度への参加と認証**

  外国税関当局のサプライチェーン保全制度で認証を取得している現行の事業提携会社または取引見込み先には、この認証取得を外国の製造業者に知らせるよう義務付けるべきです。

- **セキュリティ手続き**

  米国向け貨物について、外国の製造業者は、輸送サービスを他社に下請けに出している C-TPAT 運送会社が、事業提携会社の必要条件に概説される C-TPAT セキュリティ基準を満た

している非 C-TPAT 運送会社もしくは C-TPAT 認可運送会社を使用していることを監視すべきです。

外国の製造業者はトレーラーやコンテナへの積込みに対する責任を負うので、運送業者と協力して、積込み地点において有効なセキュリティ手続きや管理が実施されていることを確実にすべきです。

コンテナとトレーラーのセキュリティ

コンテナとトレーラーの完全性を維持し、無許可の材料及び/または人物の導入を防止しなければなりません。積込み地点では、出荷コンテナやトレーラーに適切なシールを施し、その完全性を維持する手続きを定め、実施しなければなりません。米国向けの荷積みコンテナやトレーラーにはすべてハイセキュリティ・シールをしなければなりません。すべてのシールは、ハイセキュリティ・シールの現行基準である PAS ISO 17712 と同等以上のものを使用しなければなりません。

コンテナやトレーラーに潜入者や密入国者がいないかどうか確認する必要があるハイリスク地域では、このリスクが製造施設または積込み地点で対応できるように手続きが設定されていなければなりません。

- **コンテナ検査**
  コンテナ・ドアの施錠装置の信頼性を確認するなど、コンテナ構造が物理的に完全であることを積込み前に確認する手続きが定められていなければなりません。すべてのコンテナに対して次の 7 箇所の検査プロセスを奨励します。
  - 前壁
  - 左側面
  - 右側面
  - 床面
  - 天井/屋根
  - 内部/外部ドア
  - 外部/車台

- **トレーラー検査**
  トレーラー・ドアの施錠装置の信頼性を確認するなど、トレーラー構造が物理的に完全であることを積込み前に確認する手続きが定められていなければなりません。すべてのトレーラーに対して次の検査プロセスを奨励します。

- 第5輪部分 - コンパートメント/スキッドプレートが自然な常態かどうかチェックする
  - 外部 - 前/横
  - 後部 - バンパー/ドア
  - 前壁
  - 左側面
  - 右側面
  - 床面
  - 天井/屋根
  - 内部/外部ドア
  - 外部/車台

- **コンテナとトレーラーのシール**
  トレーラーやコンテナのシールの完全性が維持されるようなシールを装着することは、サプライチェーン保全における非常に重要な要素であるとともに、C-TPATにおける外国の製造業者の重要なコミットメントでもあります。外国の製造業者は米国向け積載済みトレーラー及びコンテナのすべてにハイセキュリティシールを装着しなければなりません。すべてのシールは、ハイセキュリティシールの現行基準であるPAS ISO 17712と同等以上のものを使用しなければなりません。

  文書化された手続きには、積載済みコンテナやトレーラーへのシール装着方法及びシール管理方法が規定され、また改ざんや侵害されたシールを検知し、それを米国税関国境保護局(CBP)または適切な外国政府当局へ通報する手続きが含まれていなければなりません。セキュリティ保護のため、シールを配布するのは指定された従業員だけに限定すべきです。

- **コンテナやトレーラーの保管**
  外国の製造業者の管理下又はその施設内にあるコンテナやトレーラーは、不法アクセスや操作を防止するために安全な場所に保管しなければなりません。コンテナやトレーラー、あるいはその保管場所への不法侵入を通報し、それを安全処理するための手続きも定めなければなりません。

物理的アクセス管理

アクセス管理は、施設への不法侵入を防止し、従業員や訪問者を管理するとともに、会社資産を保護します。アクセス管理には、すべての入口地点における従業員や訪問者、業者の全員に対する確実な身元確認が含まれなければなりません。

- **従業員**
  確実な身分証明書の確認とアクセス管理のために、従業員身分証明制度を実施し、従業員にはその業務遂行に必要な保全区域へのみアクセスを与えるべきです。会社経営陣または警備職員は、従業員や訪問者、業者の身分証明バッジの発行･回収について適切な管理体制を敷かなければなりません。(鍵、キーカードなどの)アクセスデバイスの発行、回収、変更の手続きは文書化されていなければなりません。

- **訪問者**
  訪問者記録に残す目的上、訪問者は到着時に写真付き身分証明書を提示しなければならず、また、すべての訪問者は従業員に同行され、訪問者用の身分証明書が見えるように表示しなければなりません。

- **配達 (郵便配達を含む)**
  記録維持の目的上、すべての配達業者は到着時に適切な業者身分証明書及び/または写真付き身分証明書を提示しなければなりません。到着した小包や郵便は、それを配布する前に定期的に検査すべきです。

- **無許可の人物(侵入者)の撤去**
  無許可または未確認の人を識別し、これに対応するための手続きを実施しなければなりません。

<u>**従業員セキュリティ**</u>

応募者を審査し、現在働いている従業員を定期的にチェックするためのプロセスを実施しなければなりません。

- **雇用前の身元確認**
  職歴や照会先などの応募採用情報を雇用前に確認しなければなりません。

- **バックグラウンドチェックと調査**
  外国の規制に矛盾しない範囲で、採用予定の従業員のバックグラウンドチェックや調査を実施することが必要です。雇用後は、従業員の地位や役職の内容や重要性に応じて、あるいはその理由が生じた場合に、定期的にチェックと再調査が行われるべきです。

- **雇用終了手続き**
  会社は雇用終了したか解雇された従業員から施設やシステムへのアクセスを撤回し、身分証明書を回収する手続きを定めなければなりません。

業務手続きのセキュリティ

サプライチェーンにおける貨物の運送、取扱、保管に関するプロセスの完全性と保全を確実にするセキュリティ対策が実施されなければなりません。

- **文書処理**
  商品/貨物の通関過程で利用されるすべての情報が読みやすく、完全で正確であること、そして情報の入替え、喪失、不正確な情報の導入から保護されていることを確保する手続きを実施しなければなりません。文書管理にはコンピュータアクセスと情報の保護が含まれていなければなりません。

- **マニフェスト手続き**
  貨物の完全性を保証するために、事業提携会社から受け取った情報が適時、正確に報告されることを確実にするための手続きが実施されなければなりません。

- **出荷･受取**
  出発貨物は貨物マニフェストの情報と一致していることが確認され、また、貨物の内容が正確に記述され、かつ記載された重量、表示ラベル･マーク、及び数量が一致していることが検証されなければなりません。出発貨物は注文書または荷渡し指図書とつき合わせて確認し、貨物の受取または引渡し前には、貨物の配達･受取をする運転手の身分証明書を確実に確認しなければなりません。さらに、入荷及び出荷貨物が適時に移動していることを追跡するための手続きを確立しなければなりません。

- **貨物の不一致**
  貨物の不足･過剰、その他の重要な不一致または異常は、適切に調査･解決されなければなりません。異常、あるいは違法活動もしくはその疑いがある活動が発見された場合は、必要に応じて税関及び/または適切な取締当局に通報しなければなりません。

物理的セキュリティ

国際的地域の場合、貨物取扱・保管場所には不正アクセスを防止する物理的障壁(バリア)と妨害物が設けられていなければなりません。外国の製造業者は、自社のサプライチェーン全体において適宜、以下のような C-TPAT の物理的セキュリティ基準を取り入れるべきです。

- **フェンス**
  貨物取扱場所と保管場所の周囲をフェンスで囲む。国内貨物、国際貨物、高額貨物、危険貨物を分離区別するために、貨物取扱い場所内に内部フェンスを使用する。フェンスは完全性を確認し破損発見のために定期的に検査する。

- **ゲートと検問所**
  車両や人が出入するゲートには警備員を配置するか、監視装置を配備する。適切なアクセスと安全確保のため、ゲートの数はできるだけ少なくする。

- **駐車**
  私用の乗用車は、貨物取扱・保管場所の中または近くに駐車することを禁止する。

- **建物構造**
  建物は不法侵入に耐える素材で建築され、定期的な点検と修理を行い建物構造を完全な状態に維持する。

- **施錠装置と鍵の管理**
  外部及び内部の窓、ゲート、フェンスには施錠装置を用いて厳重に閉鎖され、すべてのロックと鍵の発行は経営陣または警備担当者が管理する。

- **照明**
  出入口、貨物取扱· 保管場所、フェンス、駐車場などを含め、施設の内外に十分な照明を提供する。

- **警報装置とビデオ監視カメラ**
  運送業者のリスクアセスメントによって適切に判断された場所に警報装置やビデオ監視カメラを設置して敷地内を監視するとともに、貨物取扱· 保管場所への不正侵入を防止する。

情報処理に関するセキュリティ

- **パスワード保護**
  情報システムは個人個人に独自のアカウントを割り当てて、パスワードの定期的変更が必要な仕組みでなければなりません。IT セキュリティの方針、手続き、及び基準が定められており、それらは訓練を通して従業員に提供されなければなりません。

- **責任所在の明確化**
  不正なアクセス、業務データの改ざん· 修正など、IT の乱用や誤用を判別するシステムを設置し、システムへの違反行為を働いた人にはその誤用· 乱用に見合った懲罰を与えなければなりません。

セキュリティの訓練· 教育と意識向上

テロリストや密輸業者の脅威に対する意識向上を図るための脅威に対する意識向上プログラムは、セキュリティ管理担当者によって確立され維持されなければなりません。また、従業員には、状況へ対応し報告するための社内手続きがあることを知らせなければなりません。出荷/受取場所の従業員、及び郵便物の受取と開封を担当する従業員には追加の訓練を提供しなければなりません。

また、貨物の完全性の維持方法、内部の共謀· 陰謀の見分け方、アクセス管理の保護方法などについて、従業員を支援する特定の訓練を提供すべきです。そしてこのプログラムには積極的に取組む従業員に対するインセンティブ提供が盛り込まれているべきです。